



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/655,297	09/05/2000	Ram Pemmaraju	PNE-203	8146

7590

04/29/2004

Siegmar Silber Esq
Silber & Fridman
66 Mount Prospect Avenue
Clifton, NJ 07013-1918

EXAMINER

TRUONG, THANHNGA B

ART UNIT PAPER NUMBER

2135

DATE MAILED: 04/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/655,297

Applicant(s)

PEMMARAJU, RAM

Examiner

Thanhnga Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 February 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) The invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Tuai (US 5,153,918).

a. Referring to claim 1:

i. Tuai teaches:

(1) a security computer adapted to receive said demand for access together with said login identification and to communicate with said host computer and with said associated telephonic device of said accessor **[i.e., the central access controller receives an encrypted control signal corresponding to at least a portion of an orally generated speech pattern of a prospective users from a transponder disposed at least one of any number of remote location. A voice verification unit is also included as part of the central access controller for comparing the compressed digital signal with a stored signal unique for each designated user of the system in order to permit access to the host computer if the signals compared are indeed identical. As shown in Figure 1, the controller 15 is interconnected between the host computer 10 and the modem 12 thereat while each transponder 16 is interconnected between a user terminal 11 and the modem 13 thereat (column 3, lines 4-15 and column 4, lines 2-5)];**

(2) a callback device operable in response to instructions from said security computer to call the accessor **[i.e., the capabilities of the central access controller 15 also include the optional call-back measure to enhance the security of the communication system. With this, the central access controller**

15 can be equipped with a single incoming line and at least one outgoing line. The incoming line is used for answering calls from one or more transponders 16 and each outgoing line is used to call back the designated user after verification (column 8, lines 3-10)];

(3) a subscriber database addressable by the security computer for retrieval of telephone numbers corresponding to said login identification [i.e., **The central access controller 15 is equipped to store pre-programmed telephone numbers for designated users, or to prompt the user to enter a telephone number to be used for a call back operation after verification (column 8, lines 11-14)];**

(4) said security computer adapted to provide callback instructions to said callback device to connect said associated telephonic device of said accessor to said security computer [i.e., **When not being used for programming or access to the host computer 10, the controller 15 has a display 27 which is programmed to indicate the status of each of the communications lines of the controller 15. The status shows the length of time a user has been logged on, the time of log on, the number called (if programmed to use call back security), and other pertinent information so required (column 7, lines 17-25)];**

(5) prompt means for instructing said accessor to re-enter predetermined data at and retransmit predetermined data from said associated telephonic device to said out-of-band security system [i.e., **the security system can be programmed to require a prospective user to repeat the required words up to three times. The controller 15 prompts the user to speak without providing the user with the specific words to be uttered as an additional security measure (column 8, lines 44-49)];**

(6) comparator means in said security computer for authenticating access demands in response to retransmission of predetermined data from said associated telephonic device of said accessor [i.e., **voice verification usually involves a comparison of fixed speech templates to an inputted voice pattern with possible secondary or tertiary analyses performed if the comparison**

Art Unit: 2135

yielded marginal differences in the patterns. Voice verification, as embodied in the present system, requires the user to speak from one to five words into a microphone or speaker 21 which is part of the transponder device 16 (column 1, lines 54-58 and column 8, lines 39-44)]; and,

(7) said security computer, upon verifying a match between said predetermined data and the re-entered and retransmitted data, providing authentication of the accessor and instructing the host computer to grant access thereto [i.e., the central access controller includes an encrypter/decrypter device to decrypt the received encrypted signal. A voice verification unit is also included as part of the central access controller for comparing the compressed digital signal with a stored signal unique for each designated user of the system in order to permit access to the host computer system if the signals compared are indeed identical (column 3, lines 8-15)].

b. Referring to claim 2 which depends on claim 1:

i. Tuai further teaches:

(1) said callback device is a telephone; said associated telephonic device of said accessor is a tone generating instrument with a keypad for entering data; and, said prompt means is an auditory message describing data to be entered [i.e., the capabilities of the central access controller 15 also include the optional call-back measure to enhance the security of the communication system. With this, the central access controller 15 can be equipped with a single incoming line and at least one outgoing line. The incoming line is used for answering calls from one or more transponders 16 and each outgoing line is used to call back the designated user after verification (column 8, lines 3-10). The central access controller 15 is equipped to prompt the user to enter a telephone number to be used for a call back operation after verification (column 8, lines 11-14). The inventor mentioned above the use of the telephone lines, which inherently can be used for the traditional telephone including keypad].

c. Referring to claim 3 which depends on claim 2:

i. Tuai further teaches:

(1) an announcement database therewithin; and a voice module capable of selecting a prerecorded auditory message from said announcement database and, for prompting the entry of data by said accessor, playing said prerecorded auditory message over said telephone [i.e., **The central access controller 15 is equipped to store pre-programmed telephone numbers for designated users, or to prompt the user to enter a telephone number to be used for a call back operation after verification (column 8, lines 11-14)).**

d. Referring to claim 4 which depends on claim 3:

i. Tuai further teaches:

(1) upon attaining an access-granted condition said security computer communicates the status to said accessor by selecting and transmitting an access-granted message from said announcement database and sequentially disconnecting from the connection with said telephone [i.e., **when the call to the central access controller 15 is answered by the controller modem 12, the controller 15 polls the caller looking for the proper automatic response from the transponder 16. If the transponder 16 does not respond, the call is terminated by the controller 15. Once access is granted, the controller 15 commands the transponder 16 to request identification from the user. It is here that the user provides the proper keystrokes (ASCII input) and/or speech and/or other identification (column 6, lines 40-53)).**

e. Referring to claim 5 which depends on claim 2:

i. Tuai further teaches:

(1) a voice module, in response to instructions from said security computer, capable of synthesizing an auditory message, and, for prompting the entry of data by said accessor, playing a synthesized auditory message over said telephone [i.e., **the transponder digitizer 18 is an analog-to-digital converter, a device which converts analog signals to digital signals and is used specifically in this computer access security system to receive the analog signal corresponding to spoken word(s) of designated users. The analog-to-digital converter 18 may be a CODEC design with 12 bit accuracy, encoding 12 bits of data into 8 bits of data**

Art Unit: 2135

with negligible loss of voice data. As a side benefit from the use of the CODEC device, the transponder 16 is capable of speech playback as well as speech prompts to the user (column 5, lines 22-32)].

f. Referring to claim 6 which depends on claim 5:

i. This claim has limitations that is similar to those of claims 3 and 4 , thus it is rejected with the same rationale applied against claims 3 and 4 above.

g. Referring to claim 7 which depends on claim 1:

i. Tuai further teaches:

(1) a voice recognition program operating in response to instructions from said security computer to authenticate the accessor [i.e., the central access controller includes an encrypter/decrypter device to decrypt the received encrypted signal. A voice verification unit is also included as part of the central access controller for comparing the compressed digital signal with a stored signal unique for each designated user of the system in order to permit access to the host computer system if the signals compared are indeed identical (column 3, lines 8-15)];

(2) a speech database addressable by the security computer for retrieval of a speech sample of an accessor corresponding to the login identification of said accessor, said computer adapted to provide instructions to connect and disconnect said security computer to and from said associated telephonic device of said accessor [i.e., the security system uses a voice verification unit which allows for updates of speech templates found in the controller subsequent to each authorized access to the host computer by a designated user. System operator interface is not required for speech template updating as the process is automatic. As each inputted speech pattern is compared to existing patterns contained in the templates and found to match within preprogrammed tolerances, the inputted speech pattern is either substituted for the existing pattern on combined in a predetermined manner with the existing pattern to produce a new, updated template (column 3, lines 20-31)];

(3) voice sampling means for instructing said accessor to repeat back and transmit a predetermined auditory statement over said associated telephonic device to said security computer **[i.e., voice verification, as embodied in the present system, requires the user to speak from one to five words into a microphone or speaker 21 which is part of the transponder device 16. The security system can be programmed to require a prospective user to repeat the required words up to three times (column 8, lines 39-46)];**

(4) voice recognition means in said security computer for authenticating access demands in response to transmission of said predetermined auditory statement received over said associated telephonic device of said accessor **[i.e., the function of the controller 15 is to receive all incoming calls and to verify voice, passwords or other identification means (column 6, lines 56-58)];** and,

(5) said security computer, upon authenticating a match between the predetermined auditory statement and the transmitted voice data, providing authentication of the accessor and instructing the host computer to grant access **[i.e., A voice verification unit is also included as part of the central access controller for comparing the compressed digital signal with a stored signal unique for each designated user of the system in order to permit access to the host computer system if the signals compared are indeed identical (column 3, lines 10-15)].**

h. Referring to claim 8:

i. Tuai teaches:

(1) interception means for receiving and verifying said identification number and password **[i.e., receive all incoming calls and to verify voice, passwords or other identification means (column 6, lines 56-58)];**

(2) a security computer receiving from said interception means said verification of said accessor together with said identification number thereof, said security computer structured to communicate with said web server and with said telephonic device associated with said accessor, said computer adapted to provide instructions to connect and disconnect said security computer to and from said associated telephonic device of said accessor **[i.e., a voice verification unit is also**

included as part of the central access controller for comparing the compressed digital signal with a stored signal unique for each designated user of the system in order to permit access to the host computer system if the signals compared are indeed identical (column 3, lines 10-15));

(3) an authentication program means, operating out-of-band of said web server, for authenticating an individual demanding access to said web server [i.e., the function of the controller 15 is to receive all incoming calls and to verify voice, passwords or other identification means (column 6, lines 56-58)];

(4) a biometric analyzer operating in response to instructions from said authentication program means to analyze a monitored parameter of said individual [i.e., each attempted access results in the speech verification unit 24 receiving the latest version of the compressed signal corresponding to at least one spoken word (column 6, lines 2-5)];

(5) a biometric parameter database addressable by the biometric analyzer for retrieval of a previously registered sample of said individual, said sample corresponding to the identification number of said accessor [i.e., the transponder 16 also houses at least one speech template 22 such that the compressed signal can be stored in the speech template 23 prior to being encrypted in the encrypter/decrypter device 19. The speech template 22 is an integral part of the transponder 16 and the entire modem security communication system as it contains the latest version of the compressed signal corresponding to at least one spoken word. This compressed signal is sent from the speech template 22 to the encrypter/decrypter 19 as soon as practicable after the spoken word is uttered. Such is then passed to the controller 15 for a comparison of the compressed signal with a previous digital signal stored in the controller 15. The comparison is performed in a speech verification unit 24 located in the controller 15 (column 5, lines 40-54)];

(6) sampling means for instructing said accessor to provide and transmit a predetermined entry of said monitored parameter over said associated telephonic device to said biometric analyzer [i.e., functionally, transponder

Art Unit: 2135

16 exists to transmit the data used for identification to the central access controller 15. When voice verification is used, the transponder 16 will digitize an analog signal corresponding to a spoken word, compress that digitized signal to a predetermined byte sequence and transmit the compressed signal via the transponder modem 13 to the central access controller 15 after passing through the encrypter/decrypter device 19 (column 5, lines 55-63)];

(7) **comparator means in response to a matching analysis between the characteristics of said sample and of said transmission of said predetermined entry of said individual for providing authentication to said security computer [i.e., Signal is then passed to the controller 15 for a comparison of the compressed signal with a previous digital signal stored in the controller 15. The comparison is performed in a speech verification unit 24 located in the controller 15 (column 5, lines 50-54)]; and,**

(8) **said security computer, upon authenticating a match between to the predetermined entry and the sample, providing authentication of the accessor and instructing the web server to grant access [i.e., each attempted access results in the speech verification unit 24 receiving the latest version of the compressed signal corresponding to at least one spoken word. The controller memory 26 on the other hand receives the stored digital signal corresponding to the same spoken word but it receives this after access is allowed to the host computer. The effect of such an arrangement is to compare a prospective user's utterance with his own last utterance used to gain access to the system (column 6, lines 2-11)].**

i. Referring to claim 9 which depends on claim 8:

i. Tuai further teaches:

(1) **said authentication program is a voice recognition program, said biometric analyzer is a speech pattern analyzer, and said monitored parameter is a speech pattern of said individual [i.e., the security system uses a voice verification unit which allows for updates of speech templates found in the controller subsequent to each authorized access to the host computer by a**

designated user. System operator interface is not required for speech template updating as the process is automatic. As each inputted speech pattern is compared to existing patterns contained in the templates and found to match within preprogrammed tolerances, the inputted speech pattern is either substituted for the existing pattern or combined in a predetermined manner with the existing pattern to produce a new, updated template (column 3, lines 20-31)].

j. Referring to claim 10 which depends on claim 9:

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

k. Referring to claim 11 which depends on claim 10:

i. This claim has limitations that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

l. Referring to claim 12 which depends on claim 10:

i. This claim has limitations that is similar to those of claim 7 (3), thus it is rejected with the same rationale applied against claim 7 (3) above.

m. Referring to claim 13:

i. This claim has limitations that is similar to those of claims 1, 2, and 3, thus it is rejected with the same rationale applied against claims 1, 2, and 3 above.

n. Referring to claim 14 which depends on claim 13:

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

o. Referring to claim 15 which depends on claim 14:

i. This claim has limitations that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

p. Referring to claim 16 which depends on claim 13:

i. This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

q. Referring to claim 17 which depends on claim 16:

i. This claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

r. Referring to claims 18 and 19:

i. This claim has limitations that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

Response to Argument

3. Applicant's arguments filed February 11, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

"In Tuai '918, there is no in-band/out-of-band distinction as the process takes place totally in-band. The security controller of Tuai '918 is a gatekeeper and not a device in a separate operating channel. Additionally, security functions are distributed differently, and remarkably so. In the two inventions - certain operations take place after verification in Tuai '918 which operations are compared to those of the Applicant which take place before verification. These distinctions are not subtleties, but are substantive. Not only does Tuai '918 lack the distinct channels of the Applicant, but the patent teaches away from out-of-band operation."

Examiner maintains that:

Tuai discloses all the limitation of the applicant's invention. Furthermore, Tuai teaches the security system also includes a modem at each remote location (that is out-of-band) to interact with the transponder thereat as well as a modem at the host computer location to interact with the host computer and the modems of the remote locations (column 2, lines 45-50). Moreover, Tuai further teaches The transponder is connected with the modem thereat in order to deliver the control signal thereto in encrypted form. The modem, in turn, is able to receive and transmit this encrypted control signal, for example, via telephone lines, cellular communications, microwave or other suitable transmission means, to the modem at the host location, which is constructed to receive the encrypted control signals from all the modems of the remote locations (again that is out-of-band) (column 2, lines 62-68). In addition, by definition, out-of-band (a LAN term, refers to the capacity to deliver information via

Art Unit: 2135

modem or other asynchronous connection (see Newton's Telecom Dictionary, page 582).

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

a. Newton's Telecom Dictionary (19th edition, by Harry Newton) discloses the definition of an "out-of-band" term (see page 582).

b. Coley et al (US 5, 826, 014) discloses sending an "out-of-band" system message in response to a username or username/password combination provided by a user. Such a system involves communicating a password, or password portion, back to a user on a communication medium other than the computer network being used. The user enters the information received by out-of-band means to complete a logon process. For example, a user can be prompted to enter their username and the first half of a password. The system receiving this information, upon verifying it, sends back the remaining half of the password to the user by automatically generating a phone call to a beeper provided to the user (column 12, lines 26-37).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.


Art Unit: 2135

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT

April 26, 2004


KIM VU
SUPERVISOR, EXAMINER
TECHNOLOGY CENTER 1700